

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Glen Sgambati et al

Application No.: 10/773,642

Filed: February 6, 2004

For: ACCOUNT-OWNER
VERIFICATION DATABASE

Customer No.: 20350

Confirmation No. 7640

Examiner: Gerald C. Vizvary

Technology Center/Art Unit: 3684

**DECLARATION PURSUANT TO
37 CFR § 1.131**

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

I, Glen Sgambati, declare as follows:

1. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and, further, that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the above-referenced application or a patent issued therefrom.

2. I, Glen Sgambati (the "Inventor"), am the inventor of the subject matter of the claims pending in U.S. Patent Application Serial No. 10/773,642 (the "Application").

3. I was employed by Primary Payment Systems, Inc. ("Primary Payment") during at least the time period from the conception of the invention claimed in the Application through the filing of the Application on February 6, 2004.

4. I was under a duty to assign all inventions derived from my work at Primary Payment, to Primary Payment, during at least the time from the conception of the invention through filing of the Application on February 6, 2004.

5. I understand that in a Final Office Action dated March 24, 2010 (the "Office Action"), claims 1-4, 6-13, and 17 (the "Pending Claims") were rejected as allegedly obvious over various references, including Weinflash, U.S. Patent Application No. 10/144,740 ("Weinflash"). Weinflash has since issued as U.S. Patent No. 7,383,227.

6. I understand that Weinflash was published on November 20, 2003. It is my understanding that this is the earliest date that Weinflash was published.

7. I possessed a definite and permanent idea in my mind of the inventive embodiments recited in the Pending Claims prior to November 20, 2003 and, therefore, conceived the inventive embodiments recited in the Pending Claims of the Application in the United States prior to November 20, 2003.

8. On September 12, 2003, the inventive embodiments recited in the Pending claims were disclosed to Clark A. Jablon, an attorney working on behalf of Primary Payment, in order to permit a patentability search to be conducted.

9. Attached as **Exhibit A1** are pages of handwritten notes written by Mr. Jablon during our interview of September 12, 2003 (the "Inventor Interview").

10. Based on the Inventor Interview, Mr. Jablon had a patentability search conducted by Lacasse & Associates, LLC. An email sent on September 12, 2003 by Mr. Jablon confirming this patentability search is attached as **Exhibit A2**.

11. An initial search report based on the September 12, 2003 interview was ordered by Mr. Jablon on September 22, 2003. This request is attached as **Exhibit B**. The request includes a disclosure of the claimed invention as provided to Lacasse & Associates, LLC.

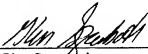
12. Mr. Jablon then completed and forwarded a patentability study on December 5, 2003 (the "Patentability Study"). The information used by Mr. Jablon and his law firm to create

the Patentability Study was obtained solely from the patentability search report and the Inventor Interview of September 12, 2003. The Patentability Study is attached as **Exhibit C**.

13. Additionally, an email from James A. Huizinga to me, dated November 29, 2002 is attached as **Exhibit D**. This email relays various aspects of the invention as I had previously disclosed to Mr. Huizinga.

Respectfully submitted,

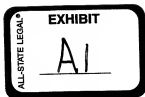
Date: 7/9/10


Glen Sgambati

62703765 v1

TCD - T. MURPHY
 - R. MARY
 - CTS

9/12/03



- developing new participant Data Base technology

- daily update of DDA acct info for advertising
 have.

↳ provide "early warning" on those records.

- closed

- ~~open~~

- hard h.t. \rightarrow \uparrow return rate

- soft \rightarrow restructure acct / new?

- informed \rightarrow new DDA / line of credit, etc.

- BANK then decides what to do w/ it --

- unless "new participant" BANK \Rightarrow see APP

* NOT generating awareness of funds *

\Rightarrow i.e. - if chkt for \$1,000,
 ht only \$ ~~1000~~ 100 n acct. --

(Direct Effect)

STATUS
 ONLY

BANK
 on
 account
 only \rightarrow

⑦ STORE ALL OF INFO FOR 10 DAYS

↳ receive Bank's orig returns (not proof)

- generate notification of return

DP
has multiple
denomin

Record check - hard h.t.s

↳ for network community

- use most current info for bank upon hard proof
- use last status provided by bank

- account is current logic

- only know type of status based on —

- don't know :
- owner
 - x
 - y
 - z

- verification of account ownership → FOR AID

- "Proof out"

- provide agency of additional validated info.

- real-time, on-line

↳ require input for response

- provide yes/no answers only for each check

↓ as two persons independent to transcribe on their
Records ~~to~~

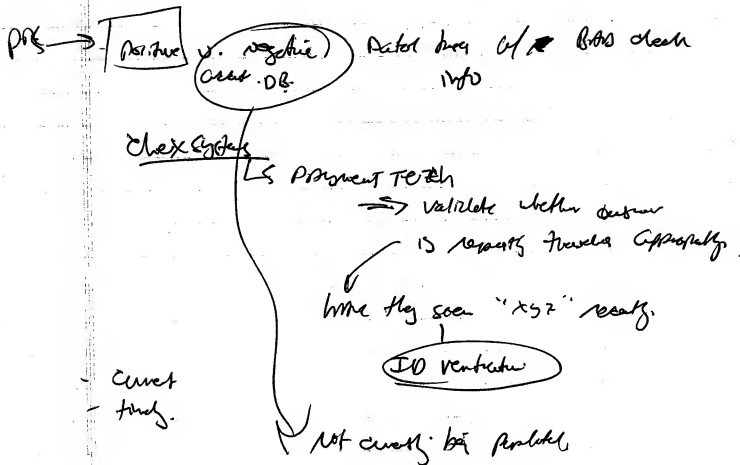
- collecting additional info for non-patient injury agency
↳ "insurance"

∴ for non-pat D.B., will at least be able
to confirm ID / address in the D.B.
⇒ won't be able to confirm
State / location of case.

based on

Statistical / historical data

- Check Acceptance Cms ~ 5 Telecheck



- established input @ POS / acceptance

- SROs
- financial institution
- direct web inquiry / input
- auto send to POS ...
- "faceless" transaction (ID is not presented)

NSD

- IF PRX partition - then will also retain state
- Whether or some of data will be provided to singer

Disclosures

- Chakrabarti - May/03
↳ user interview
- Operator Amuray - Feb/03
↳ 1st written disclosure (conspiracy)

forget lunch of 4/04
Teeny of 1/04

Red wings The Phoenix

① Verify if Re.ing or best possible a DB of parallel (not. petat) data tables for row-patient data lines.

② How differ from credit card thing?

→ Are credit cards checked of "Data checks"??

↳ doesn't this show the verification process?

① Internet purchase of cheap goods

② Many utility bill up checks over.

a) App → Customer can't pay by bill
⇒ Utility vendor accept it valid.

b) Problem → Still know what #

- ① U.P. IS Contrib. of NW. Centr. data
↳ look @ non-PPS bank

⇒ Are popularity DEEP w/ Vespert Data

- business rules around that data
↳ coded to include non-PPS data

"Vespert Data Contribution"

- 1) ~~not~~ or reliable
- 2) only what can physically see
- 3) distinction drawn ~~to~~ → not to answer
* capture as much info as possible *

* may open
Vespert to provide
distinct data *

→ (Statistical/historical analysis...) (non-PPS info)
→ Vespert captures all

- ~~not~~

- context w/ answer or to refer returned

Pay by check.com" → looks like checks --

↳ These being populated by negative Database
↓
appears to use negative info

⇒ we use positive info directly from banks.

② Credit Card - Clearence

- On-line Credit \Rightarrow 1) name \Rightarrow AUS
2) B.Ming ADDR. \Rightarrow "Address verification system"

- Look @ ST. Address + ZIP
look for full / Partial match (price differ if not used)

- AUS contributed by CC companies

* - we look @ any Info Contributed by credit network
x (WATERS)
& (CC)

\Rightarrow few steps further

- type of account \rightarrow other potential users.

- being contributed from banks
- updated on daily basis

~~they~~

* finally no limit left credit # + name at each branch
(unless in a reg. DB)

* credit ADV situation (if CC)

* Debit / checking account payment

- Multiple ^{data} fields
- DB Populated w/ ~~new~~ Patient + new patient DB

\downarrow from \downarrow new patient
- Using positing method ~~data~~

- ① - creation of DB
- 1) interview takes
 - 2) check property

f Using DB

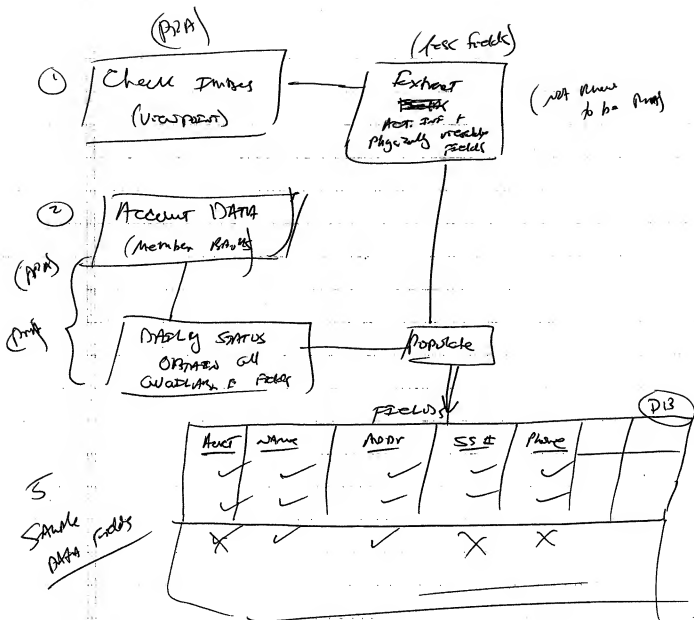
- ① Concept of Searching for fields in C. C++
appears to be known \Rightarrow by C++

- ✓ (2) VICARAGE → known to many people (Richard Purves)

- ✓ (3) REPORT CHECK - Know to have member basis
Contrib. Get. date to check STATUS of acct.

2 1/2 of all known acts, are covered.

- ✓ (4) → non-physical data
(5) PUS of credit card cos.



① DATA Base population schem

② DB OF DB \Rightarrow Return of I/O

Jablon, Clark



From: Jablon, Clark
Sent: Friday, September 12, 2003 4:51 PM
To: 'tmadison@concordefns.com'
Cc: Spicer, Andrew W.; Kasten, Leslie
Subject: Our File No.: 8850-Database elements

Dear Tanya,

Today's call was extremely productive. We learned exactly what we needed to know. In fact, we can proceed directly to a patentability search, instead of the less focused state-of-art search.

Also, given the commercial importance of the invention and the clear unmet needs that are being addressed, we will probably recommend filing unless extremely close prior art is located. We will get the search out next week with results available in mid-October.

From our conversation with Rich after you dropped off the line, the earliest possible statutory deadline appears to be February 2003 since he made his first conceptual disclosure of the idea to people outside of the company in February 2002. The first written materials were produced months later. If we go ahead with a filing, we will have it completed before the end of the year, so there will be no statutory bar problem.

-Clark

AKIN GUMP
STRAUSS HAUER & FELD LLP

Attorneys at Law

CLARK A. JABLON
215.965.1293/fax: 215.965.1210
cjabl@akingump.com



September 22, 2003

LETTER VIA FACSIMILE
CONFIRMATION COPY WITH ENCLOSURES VIA FIRST CLASS MAIL

Mr. Randy Lacasse
Lacasse and Associates
1725 Duke Street
Suite 650
Alexandria, VA, 22314

Re: Patentability Search for "Database Element Expansion Project"
Our File: 208850.0029/29US

Dear Randy:

Please conduct a patentability search on a non-rush basis with respect to the above-identified invention as described in the attached Invention Disclosure. We would like to receive the search results by October 15, 2003.

Please let us know if you have any questions. Please return all of the enclosed materials with the search results. We look forward to hearing from you shortly.

Sincerely,

CLARK A. JABLON

CAJ:AWS/lcd

Enclosures

INVENTION DISCLOSURE

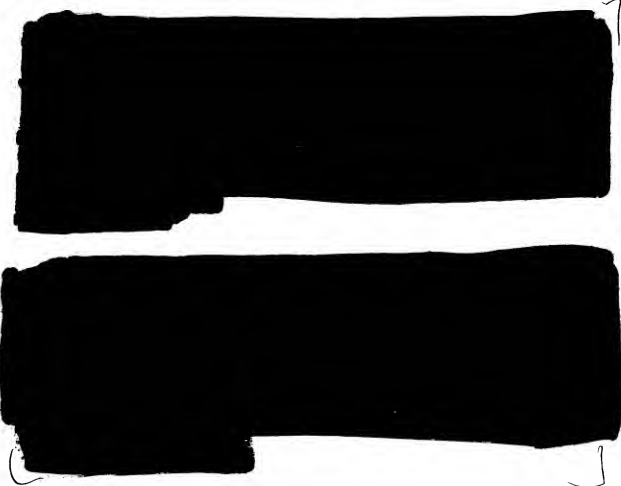
Background & Known Prior Art

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



Idea to be Searched

The accuracy and usefulness of known account verification services is directly dependant on the robustness of the information contained within the databases which those services access. For example, simply providing an inquirer with the status of the account corresponding to the check which the inquirer wants to verify does not guarantee that the consumer is actually authorized to transact on that account. Similarly, accessing the AVS for a credit card transaction only verifies the account against the known billing address – no other information about the consumer is verified.

The proposed database element expansion project ("DEEP") populates a database table as shown in the attached Fig. 1. DEEP extracts and collects data elements related to accounts at member banks based on newly opened and/or recently maintained accounts. The collected data is stored and updated daily based on additional new files sent from the

member bank to the DEEP database. For each new or updated account from a member bank, the member bank is required to provide a minimum set of data element fields: one name, one address and one social security or tax i.d. number. Other, less vital data identification fields may also be included in the file sent by the contributing member bank. The collected data elements include: names, addresses, dates of birth, identification/drivers' license numbers, social security numbers, tax i.d. numbers, account type, source origination and other various data typically associated with checking (or other) accounts. The data elements are stored in the DEEP according to the corresponding account number.

Additionally, DEEP collects and stores data corresponding to accounts from non-member banks. Non-member bank data is obtained by extracting as much information as possible from check images. Because of the limited personal information printed on paper checks, not all of the information available in DEEP for member bank contributions is collectable for non-member accounts. Accordingly, the DEEP database will not contain a full complement of data elements for non-member accounts. Additionally, non-member bank data is inherently not as reliable as member bank data. Thus, non-member bank data is noted as such in the DEEP.

As shown in Fig. 1, the sample DEEP table contains five different account entries. Data elements for accounts 789 and 432 were not obtained from a member bank, as denoted in the last field. Thus, not all of the required fields for those accounts are populated.

To use the DEEP system, an inquirer must, at the very least, provide an account number and at least one other data element field (purportedly corresponding to that account number) for verification. The inquirer may enter an account number and multiple data elements at once. Assuming that the requested account number is in the DEEP database, the requested data fields are queried against the stored information corresponding to that account. The DEEP returns a verification of each submitted data element corresponding to that account number. For each data element field in an inquiry,

a response of "yes," "no" or "information not available" is returned by DEEP to the inquirer.

No customer-specific data is provided back to the inquirer. Rather, the DEEP will only confirm or deny the accuracy of the information as entered into the data element field which corresponds to the entered account number. An example (based on Fig. 1) of a sample DEEP inquiry and response corresponding to that inquiry is shown below:

<u>Inquiry</u>	<u>Response</u>
Bank of America	
Account: 456	
Name: B. Doe	YES
Address: 20 East	YES
SS#: 987654321	NO
Phone #: 111-222-3333	INFO NOT AVAILABLE

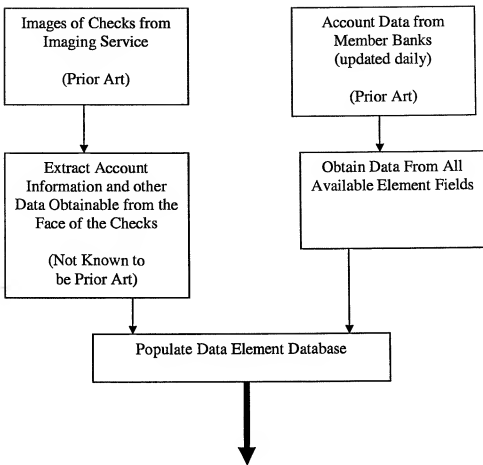
Additionally, if an inquiry regarding a particular account results in "NO" response on at least one data element in a request, DEEP reports to the member bank for that account that there was an inquiry against one of their accounts which resulted in a negative response, along with the data element (s) that produced that negative response. In the above example, a report to Bank of America would be generated that an inquiry was made against account # 456 which generated a negative response for SS#.

The DEEP provides inquiry capabilities allowing inquirers to validate information about an account holder, in addition to the account's current status. The inquiry submitted to DEEP may be made on-line, in real time or in a batch-process. Thus, the inquirer could be a major financial institution or a small business. The DEEP system is particularly advantageous for "faceless" transactions where the identity of the account holder cannot be verified. Additionally, an inquirer can determine the status and relevant account holder information about an account in real time, such that business transactions are not delayed, while still preventing fraud on the transaction.

It should also be noted that the DEEP database is positively, or actively, populated using information that is collected from actual member banks based on current account information. In contrast, other existing similar databases and account verification systems utilize negative, or passive, data based on account information which is retained based on accounts and/or checks which are known to be faulty, fraudulent or otherwise troublesome. Negatively populated databases generally contain account information for which there has been a recorded or reported problem. Since the DEEP system is utilizing a positively populated database, the status and validation of the data elements which are returned to the inquirer are both current and timely, as opposed to being based simply on databases which are populated in a haphazard manner.

Search Focus

The search should focus on the concept of populating an account verification database with data elements related to recently opened or maintained accounts as supplied by member banks. The database also contains statistically accurate account information from non-member banks. The database may be queried to verify specific data elements related to an identified account number.



Account No.	Name (required)	Address (required)	SS# (required)	Phone # (optional)	Non-Member Bank Data?
123	J. Smith	10 North Rd.	222-33-4444	123-456-7890	
456	B. Doe	20 East St.	555-66-7777		
789	R. Jones	40 West St.			YES
765	K. Johnson	30 South Ln.	888-99-0000	123-555-7777	
432	A. Gooding			345-222-1111	YES

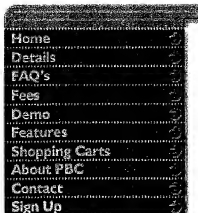
pay by check
Secure. Accurate. Reliable.



The Original "i-che

Sign Up

26 Questions



Welcome to PayByCheck!

The leading provider of electronic check processing.

PayByCheck pioneered the Internet check industry and has been continuously processing time transactions since 1997. With thousands of companies using our services we have proven platform that can securely, accurately, and reliably handle the volume of payments today's commercial sites generate.

PayByCheck allows for the payment of goods and services by check right from your web site with the industries most extensive verification, validation and even real-time biometric authentication. For call-centers, order fulfillment companies, and other high-volume clients, PayByCheck can accept batch files and process them as pre-authorized drafts or ACH settlements per NACHA rules.

PayByCheck uses your existing FDIC insured bank account and banking relationships. We do not require that your customers register with us before they can pay you. We do not limit what products or services you can sell or the dollar amounts that you can charge.



CASH **CHECKS**
According to the Federal Reserve, cash, checks are the most-used method of completing transactions.

ITI ACCOUNT #

USER NAME

PASSWORD

Login

SEARCH PAYBYCHECK:

Go

Live Help | OPEN

26 Questions to ask before selecting a check processor.

Do you mean eCheck or i-Check?

PayByCheck is the only system designed for i-Check Internet Check, transactions and includes fraud & both negative and positive databases, a proprietary address verification system and native support for biometric authentication. PayByCheck systems in Federal Regulations and NACHA banking and services.

According to the Federal Reserve, next to cash, it is the most frequently used method of completing transactions in the United States.

PayByCheck offers two account types: **Basic** (for the small to medium-sized business) **Professional** (designed for medium to large sized businesses). Both account types include access to our utilities portal where you can monitor, query and maintain your account in real time.

PayByCheck uniquely offers Electronic Check Processing (ECP) or Paper Drafts depending on your needs. ECP transactions are settled through the ACH network according to NACHA regulations. Paper Drafts are printed each day and sent to you via first class mail for deposit to your bank account.

The standard check interface is hosted on our secure servers and is accessed with simple secure, HTML links. PayByCheck can also be seamlessly integrated into your current form templates, or web site by using industry standard **XML**.



Some of Our Great Clients

Main - Details - FAQ's - Demo - Terms of Service - Signup - Utilities & About Us - Compatible Shopping Carts - Privacy Policy - Affiliate Program



ITI Internet Services, Inc. - 1130 Broadway Plaza - Tacoma, WA 98402 U.S.
Voice: 253-284-0320 Fax: 253-284-0324 E-mail: sales@paybycheck.com



Legal Notice Copyright © 1995-2003 ITI Internet Services, Inc. All rights reserved.
Check, PayByCheck and the PayByCheck logo are trademarks or registered trademarks of ITI Internet Services, Inc.

Professional accounts can customize this page.

Enter the numbers from the bottom of your check as illustrated below.

1 2 3 4 5 6 7 8 9	1 2 3 4 5 6 7 8 9 0 1 2 3
Bank Routing Code	Bank Account Number

Phone number too short, make sure to include area code

Your name as it appears on your check		Your phone number	Check number
Your address as it appears on your check		09/18/2003 01:14:46 PM	
Your city, state & zip code			
Pay To The Order Of:	Test Transactions Only	\$19.95	
	Nineteen Dollars and 95 Cents	US Dollars	
Memo	Special Order	Signature	Type your full name here
Bank Routing Code and Bank Account Number			
			Help
 This transaction is secured using the latest in encryption technology			

Enter your **email address** so that we may send you a receipt:

☐ Remember me the next time I use PayByCheck.com
(This information will be stored securely on your computer using a SubCrypted cookie)

CONTINUE

Your computer is identified as: 12.40.174.2



Customized Internet Solutions for Small Business People

Web development and consulting for your small business based on honesty,

experience, and realism. Established 1997.

Rob Taylor
(585) 367-2483
rob@tconsult.com

TConsult, Inc.

Mission

Services

History

Contact Us

Project Quote

Our Clients

Take a Demo

Internet Help

Free Newsletter

Special Thanks

For Developers

.NET Code

ASP Code

Current Newsletter Five reasons to avoid public pdf

Free Articles Is the modern going to put the fire truck out of business?

GeoTrust SSL in an Hour

Are your opt-ins being rejected by spam filters?

Address Verification System (AVS) - accept or decline

Stop forwarding chain letter hoaxes



Address Verification System (AVS) - accept or decline?

Rob Taylor - President. TConsult, Inc.

April 12, 2003

Around a year ago I was at the bait shop down the road from my house loading up for a nice afternoon of rock bass fishing in Canandaigua Lake. I know the owner quite well and we generally stike up conversation over what is new in the world. On this particular day he had mentioned that he received notice from Visa/Mastercard regarding higher fees for processing cards without entering the address associated with the card. After looking in to it myself I found he was correct. I immediately understood the reason why but also could see problems with it. The Address Verification System (AVS) has reduced online identity theft but like any system it is hardly perfect.

What is the Address Verification System (AVS)?

The Address Verification System (AVS) is an advanced level of credit card security that is now used to help guard against credit card fraud. When a card is sent to the bank for processing the house number portion of the address and postal code entered with the order must match that of the cardholder on file. This is another way to ensure that the owner of the card is in fact the one using it. If the address does not match then the transaction is declined and sent back to merchant. At that point the merchant has to decide whether to process the transaction anyway or reject it. If the merchant chooses to process the card (even though it's address is invalid) they pay a higher transaction fee. This is called an **unqualified** transaction. A transaction with an address that verifies is said to be **qualified** and the merchant is charged their normal transaction fee.

Why do we need AVS?

The answer is what you are using right now - The Internet. Since ECommerce took off in the late 1990's credit card fraud has been on the rise. Fraud was responsible for 700 million dollars in online sales losses in 2001. (Sources: **Credit Union National Association** and **CNN Sci-Tech**) The reasons range from hacking to the ease of anonymity when online. Many companies were getting burned time and again with stolen credit cards. The Address Verification System has cut down on fraud as it was intended to. As stated before, the AVS system (in most cases) does not block the card from being processed. It first gives a warning to the merchant to which the merchant must decide whether or not to proceed.

What are the pitfalls of using AVS?

Pitfall #1 - Legitimate Declines

If the address entered by the user does not match the address on file with the card then the transaction will be declined. If something is misspelled or the customer has moved the address will not verify. It is difficult to implement AVS when your customer base is Business to Business. The following scenario could happen:

Bob tells Joe to give Suzy the company credit card and rent us a car online. Suzy tries to order the car but the card is

Credit card processing and the reverse ch-ching

declined because the address on the card is wrong. What happened? Does Suzy know the company address? Did she get confused and enter her personal address instead of the billing address of the card? Is the address on the card wrong? The car company may have just lost a sale.

What is PayPal?

Spam - the deer in your headlights

Such a scenario above is highly probable. Protecting against fraud could cost you business. Then again if you process the number of transactions that an online rental car company does you would be foolish not to use AVS. The more orders you take, the more likely you will find someone using a stolen card.

Increase Search Engine Ranking

Pitfall #2 - Unqualified is not guaranteed with all banks

Some banks will not allow an unqualified transaction at all. Watch out for this. Be especially careful of this if you are buying a processing gateway (Cybercash, authorize.net, etc...) that comes with a free merchant account. The banks that offer the free merchant accounts may not accept unqualified transactions.

Data Driven Web Sites?

Should I use AVS on my web site?

It's difficult not to use it but using it could also cost you business. Like so many other decisions you will need to make about your ventures in Internet land the size of your business and who your customers are should be the determining factors in using AVS.

AVS should always be used when.....

you are selling goods on an ECommerce store. You are disconnected from these users. The crook makes a purchase, you ship it, then you find out the card was stolen. These people are extremely hard to find and law enforcement is not going to waste many resources looking for them.

AVS is not as much of an issue when.....

the services you provide are member based and the buyer must return and interact. Message boards, alumni sites, event planning sites, etc... The chances of purchases with stolen cards in this environment is small.

Remember.....

The merchant is responsible for a charge back if a fraudulent transaction happens.

Do you have any suggestions that will save me time, grief and money?

A couple. If your operation is small then you may want to consider one of the following.

Do your own verification

Turn real-time credit card processing off and manually verify your orders. Check for things in the order that may look suspicious. Call each user to confirm the order if it makes you more comfortable. Do a reverse phone number check to make sure that the phone number matches the user. You can do this at a slew of places like phonenumbers.com. Be wise to orders placed on domains that offer free mail accounts like yahoo.

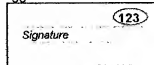
Use AVS but let declines slide through

One thing you can do when a decline occurs is to still allow the order to be completed. Then verify the card and the card holder later with your virtual terminal before you ship the product. This would even work well on a busy store. Have your web site send you an email message telling you

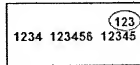
a decline has occurred. Then you can research the order and the user to see if you do in fact want to decline it (call user, email them, etc...). This should not happen often and it never gives a valid user a bad experience. You may also win loyalty by pointing out a problem to the customer that they never knew they had. Plus once the address has been corrected you can process the card at the lower fee!

Card Security Code (CSC)

Also called the Card Verification Code (CVC) or Card Identification Number (CIN). It is 3 digit number above the signature on the back of the card (4 digit on the front for American Express). If a user enters a credit card number and the CSC code is wrong - why? The card should be right there in front of them. You could use this by itself or include it with the suggestions above for further verification.



Back of Visa/MasterCard.
CSC code is circled in red.



Front of AMex with CIN
circled in red

The Future of Fighting Fraud - Payer Authentication Programs

- **Verified By Visa**
- **Mastercard SecureCode**

One way to guard against online credit card fraud is to verify with the card holding company at order time that the person using the credit card is in fact the card owner. Effective April 1, 2003 Visa and MasterCard users can assign a password to their credit card. For Visa it is called Verified By Visa and for MasterCard it will be known as Mastercard Secure Code. The Credit Union National Association (CUNA) is requiring credit unions and their Visa/MasterCard card holders to be enrolled in the program by October 1, 2003.

How does it work?

A web store enrolls in the Verified By Visa and/or MasterCard SecureCode program. When a user goes through checkout they will enter their credit card information. Upon submitting their credit card information a pop-up window will appear asking them for their password. If the password is good, the order process continues. [See a demo here.](#)

Does this eliminate AVS and having to pay higher unqualified transaction fees?

No. The bank will still want the card holder's address when you try to process the card. Visa's verification process tells the merchant that the card owner appears to be valid but it does not tell the bank that. You will still be socked with the higher transaction rate if the address on the card does not verify. However, you can be more confident than ever that the card owner is in fact the person doing the ordering. These services may also eliminate charge back liability to the merchant if a fraudulent transaction occurs. See [Credit and Debit Card issuers now responsible for fraud charges](#)

Is it free?

No. Per transaction and monthly fees apply to use the payer authentication services. Check with your processor to see if they offer it and what is costs.

More resources on this subject

2. Present Invention

The accuracy and usefulness of known account verification services is directly dependant on the robustness of the information contained within the databases which those services access. For example, simply providing an inquirer with the status of the account corresponding to the check which the inquirer wants to verify does not guarantee that the consumer is actually authorized to transact on that account. Similarly, accessing the AVS for a credit card transaction only verifies the account against the known billing address – no other information about the consumer is verified.

The proposed database element expansion project ("DEEP") populates a database table as shown in the attached Fig. 1. DEF collects data elements related to accounts at member banks based on newly op ed accounts. The collected data is stored and updated daily based om the member bank to the DEEP database. For each new o ber bank, the member bank is required to provide a minimum ; name, one address and one social security or tax i.d. number. Oth n fields may also be included in the file sent by the contributing me a elements include: names, addresses, dates of birth, identificat ers, social security numbers, tax i.d. numbers, account type, source origination and other ... data typically associated with checking (or other) accounts. The data elements are stored in the DEEP according to the corresponding account number.

COPY

Additionally, DEEP collects and stores data corresponding to accounts from non-member banks. Non-member bank data is obtained by extracting as much information as possible from check images. Because of the limited personal information printed on paper checks, not all of the information available in DEEP for member bank contributions is collectable for non-member accounts. Accordingly, the DEEP database will not contain a full complement of data elements for non-member accounts. Additionally, non-member bank data is inherently not as reliable as member bank data. Thus, non-member bank data is noted as such in the DEEP.

As shown in Fig. 1, the sample DEEP table contains five different account entries. Data elements for accounts 789 and 432 were not obtained from a member bank, as denoted in the last field. Thus, not all of the required fields for those accounts are populated.

To use the DEEP system, an inquirer must, at the very least, provide an account number and at least one other data element field (purportedly corresponding to that account number) for

verification. The inquirer may enter an account number and multiple data elements at once. Assuming that the requested account number is in the DEEP database, the requested data fields are queried against the stored information corresponding to that account. The DEEP returns a verification of each submitted data element corresponding to that account number. For each data element field in an inquiry, a response of "yes," "no" or "information not available" is returned by DEEP to the inquirer.

No customer-specific data is provided back to the inquirer. Rather, the DEEP will only confirm or deny the accuracy of the information as entered into the data element field which corresponds to the entered account number. An example (based on Fig. 1) of a sample DEEP inquiry and response corresponding to that inquiry is shown below:

Inquiry

Response

Bank of America

Account: 456

Name: B. Doe

Address: 20 East

SS#: 987654321

Phone #: 111-222-3333

YES

YES

NO

INFO NOT AVAILABLE

Additionally, if an inquiry regarding a particular account results in "NO" response on at least one data element in a request, DEEP reports to the member bank for that account that there was an inquiry against one of their accounts which resulted in a negative response, along with the data element (s) that produced that negative response. In the above example, a report to Bank of America would be generated that an inquiry was made against account # 456 which generated a negative response for SS#.

The DEEP provides inquiry capabilities allowing inquirers to validate information about an account holder, in addition to the account's current status. The inquiry submitted to DEEP may be made on-line, in real time or in a batch-process. Thus, the inquirer could be a major financial institution or a small business. The DEEP system is particularly advantageous for "faceless" transactions where the identity of the account holder cannot be verified. Additionally, an inquirer can determine the status and relevant account holder information about an account in real time, such that business transactions are not delayed, while still preventing fraud on the transaction.

The DEEP database is positively, or actively, populated using information that is collected from actual member banks based on current account information. In contrast, other existing similar databases and account verification systems utilize negative, or passive, data based on account information which is retained based on accounts and/or checks which are known to be faulty, fraudulent or otherwise troublesome. Negatively populated databases generally contain account information for which there has been a recorded or reported problem. Since the DEEP system is utilizing a positively populated database, the status and validation of the data elements which are returned to the inquirer are both current and timely, as opposed to being based simply on databases which are populated in a haphazard manner.

Patent Search

The search was conducted among subsisting and expired U.S. Patents and published applications located in the publicly available files of the U.S. Patent & Trademark Office ("PTO"). U.S. patents and published applications in the following classes/subclasses were reviewed:

Classification Search

<u>Class</u>	<u>Subclass</u>	<u>Description</u>
235/		REGISTERS
	379	. Banking Systems
	380	. Credit or identification card systems
705/		DATA PROCESSING: FINANCIAL, BUSINESS PRACTICE, MANAGEMENT, OR COST/PRICE DETERMINATION
	1	AUTOMATED ELECTRICAL FINANCIAL OR BUSINESS PRACTICE OR MANAGEMENT ARRANGEMENT
	14	. Distribution or redemption of coupon, or incentive or promotion program
	35	. Finance (e.g., banking, investment or credit)
	39	.. Including funds transfer or credit transaction
	42	... Remote banking (e.g., home banking)
	44	... Requiring authorization or authentication
	45	... With paper check handling

Bill H. Abney, Esquire
Page 6
December 5, 2003

64	. Secure transaction (e.g., EFT/POS)
67	... Including authentication
75	.. Transaction verification

The integrity of the search is based on the records as presented to us by the PTO. No further integrity studies were performed. Also a key word search was performed on the PTO full-text database.

The following U.S. patent documents were identified in the search conducted by the searcher.

U.S. Patent No.

Inventor

5,404,488	Kerrigan et al.
5,832,464	Houvener et al.
6,189,785 B1	Lowery
6,351,735 B1	Deaton et al.

**U.S. Patent Application
Publication No.**

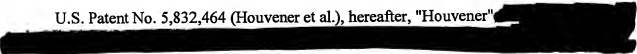
Inventor

2002/0052852 A1	Bozeman
2002/0103756 A1	Andrews et al.
2003/0130919 A1	Templeton et al.

Copies of these references above were previously sent to you and thus no additional copies are enclosed.


Discussion Of References

U.S. Patent No. 5,832,464 (Houvener et al.), hereafter, "Houvener"

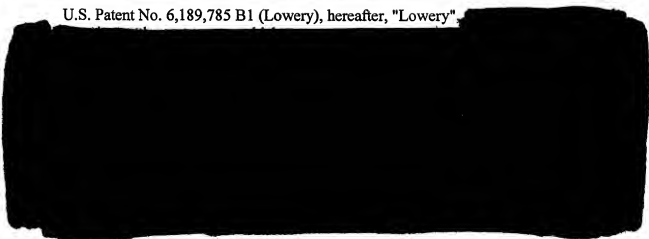


Bill H. Abney, Esquire
Page 7
December 5, 2003

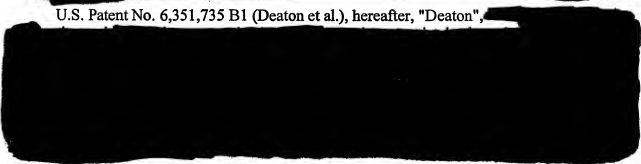
disclosed by Houvener, "1"



U.S. Patent No. 6,189,785 B1 (Lowery), hereafter, "Lowery"



U.S. Patent No. 6,351,735 B1 (Deaton et al.), hereafter, "Deaton",



Bill H. Abney, Esquire
Page 8
December 5, 2003

U.S. Patent Application Publication No. 2002/0103756 A1 (Andrews et al.), hereafter, "Andrews", [REDACTED]

The remaining patent references were deemed relevant insofar as they relate to check transaction processing. However, none of these references appear to include anything of greater significance than the references described above.

U.S. Patent No. 5,404,488 (Kerrigan et al.) [REDACTED]

U.S. Patent Application Publication No. 2002/0052852 A1 (Bozeman) [REDACTED]

U.S. Patent Application Publication No. 2003/0130919 A1 (Templeton et al.) [REDACTED]

Each of the above-identified references should be carefully reviewed to confirm our understanding and analysis.

Patentability Opinion

None of the prior art references describe an account verification database for verifying whether a person is authorized to transact on an account, where the database is populated with specific data elements corresponding to recently opened or maintained accounts as supplied and automatically updated by member banks and where the database also includes similar data elements obtained from checks drawn on non-member banks. [REDACTED]

December 5, 2003

[REDACTED] The references also do not describe querying such a database in the manner of the present invention to verify specific data elements related to an identified account number. Accordingly, it is our opinion, based on the prior art found in the search, that patent protection is likely to be available for this invention.

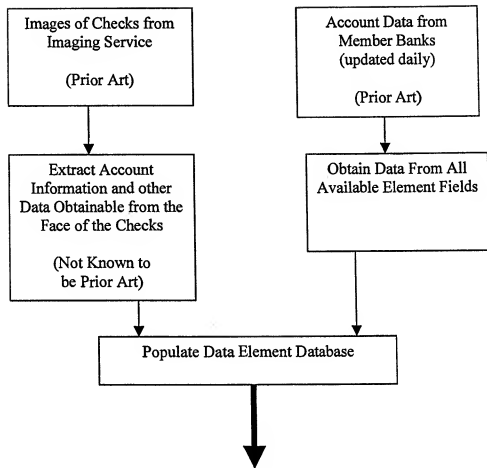
To obtain a patent, the PTO makes a determination of whether or not the invention is anticipated by (*i.e.*, the same as) or obvious in view of prior patents and other prior art references. If the invention is shown in or obvious from the prior patents and references, it is generally not patentable. In determining whether an invention is obvious, Patent Examiners are permitted to combine features from different patents and references if the combination would be obvious to one of ordinary skill in the applicable art.

[REDACTED]

Caveats

This report is based upon the disclosure made to us, as summarized above, and is the result of a limited novelty search in the publicly available files among prior U.S. patents and published U.S. patent applications in those classifications of the PTO in which, in the judgment of our searcher, the most pertinent references were likely to be found. No patent search can ever be considered to be exhaustive due to a number of factors, including varying opinions as to where the most pertinent prior art patents may be classified in the PTO search files, patents which may be missing from the search files, and reasonable limitations on time and expenditures for the search.

Additionally, with some exceptions, it is possible to search published pending U.S. patent applications where the applications were filed on or after November 29, 2000, or any previously filed applications that were requested by the applicant to be published after that date. Unless early publication is requested, it is still too early to see many patent applications published in due course, since the publication date is about 18 months from the earliest priority application relied upon for a subject application filed on or after November 29, 2000. Moreover, patent applications filed before November 29, 2000, and certain U.S. patent applications filed after that



Account No.	Name (required)	Address (required)	SS# (required)	Phone # (optional)	Non-Member Bank Data?
123	J. Smith	10 North Rd.	222-33-4444	123-456-7890	
456	B. Doe	20 East St.	555-66-7777		
789	R. Jones	40 West St.			YES
765	K. Johnson	30 South Ln.	888-99-0000	123-555-7777	
432	A. Gooding			345-222-1111	YES

IG. 1

Bill H. Abney, Esquire
Page 10
December 5, 2003

date that the applicants have indicated are not intended for foreign filing, are still retained in secrecy until a patent issues, unless the applicant specifically requests publication of such applications. The average pendency period from the filing of an application until a patent issues is about two years.

The question of whether any product or process based on the present invention would infringe an unexpired patent is beyond the scope of the present patentability search report and opinion, and has not been considered by us.

Please contact us if you have any questions or wish to discuss this matter further.

Sincerely,

CLARK A. JABLON

CAJ:AWS/lcd
Enclosure

12/5



CLARK A. JABLON
215.965.1293/fax: 215.965.1210
clablon@akingump.com

December 5, 2003

***PRIVILEGED ATTORNEY-CLIENT
COMMUNICATION-NOT TO BE
REPRODUCED OR DISCLOSED***

Bill H. Abney, Esquire
Senior Counsel
Concord EFS, Inc.
5775 Summer Trees Drive
Memphis, TN 38134

Re: Patentability Study for "Database Element Expansion Project"
Our File No. 208850.0029/29US

Dear Bill:

Pursuant to your company's request, we have conducted a patentability study for the above-identified invention and report our findings below:

Summary

It is our opinion, based on the results of the search, that patent protection is likely to be available for a method of implementing an account verification database for verifying whether a person is authorized to transact on an account, where the database is populated with specific data elements corresponding to recently opened or maintained accounts as supplied and automatically updated by member banks and where the database also includes similar data elements obtained from checks drawn on non-member banks. The process of querying such a database to verify specific data elements related to an identified account number is also likely to be patentable.

Disclosure

1. General Background of the Art

[REDACTED]

Bill H. Abney, Esquire
Page 2
December 5, 2003

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Spicer, Andrew W.

ALL-STATE LEGAL

EXHIBIT

D

From: Mayo, Rich [rmayo@primarypayments.com]
Sent: Monday, January 12, 2004 3:50 PM
To: Spicer, Andrew W.
Subject: FW: Additional Data Elements Project - FAQ's

Importance: High



603957_21_doc
(92 KB)

-----Original Message-----

From: Mayo, Rich
Sent: Monday, January 12, 2004 12:23 PM
To: Abney, Bill; Andrew W. Spicer (E-mail)
Subject: FW: Additional Data Elements Project - FAQ's

FAQ's form Legal for the project to address anticipated participant questions/concerns.

-----Original Message-----

From: Glen Sgambati
Sent: Friday, December 20, 2002 11:10 AM
To: Rich Mayo
Subject: FW: Additional Data Elements Project

-----Original Message-----

From: Huizinga, James A. [mailto:jhuizinga@sidley.com]
Sent: Friday, November 29, 2002 7:45 AM
To: 'gsgambati@primarypayments.com'
Cc: 'Lgomez-wilkins@PrimaryPayments.com'; 'PPastreich@netEPS.com'; O'Keefe, Patrick K.
Subject: Additional Data Elements Project

Glenn:

Attached is a draft set of FAQs for the Additional Data Elements Project ("Project"). Please let us know if it addresses the topics that you think will come up in discussions with Participants. Also, as you review the draft, please consider the following.

As we understand the Project, Primary Payment Systems ("PPS") would modify the Deposit Check program so that participants that contribute information on deposit accounts held by the participants ("Contributors") would also report the names, social security numbers, addresses, telephone numbers, and drivers license numbers ("Additional Data") for the individuals who opened the deposit accounts. This information is collected by the Contributor as part of the new account opening process and would be updated by the Contributor as the Contributor's records with respect to the deposit account are updated.

The Additional Data would be added to PPS's National Shared Account Database ("NASD") that contains data on deposit accounts held by the Contributors. Additional Data would not be reported by Contributors as part of "non-participant data" collected by PPS (i.e. when a Contributor provides data on deposit accounts that are not maintained by the Contributor) and Additional Data would not be included in the "non-participant database," which is maintained separately from the NASD.

The primary benefit of including the Additional Data is that it assists a user in determining whether an individual who is attempting to provide a check or initiate an ACH transaction with respect to a deposit account is an authorized user of the deposit account. The Additional Data would be especially useful to users who are participating in non-face to face transactions, such as transactions over the internet or telephone. Users expected to be interested in the Additional Data include retailers and payment processors that are initiating ACH and check transactions over the internet and telephone.

PPS would not provide the Additional Data to a user. Rather, the user would submit to PPS the relevant identifying information (e.g. name, address, social security number, etc.) and PPS would either (1) indicate whether that information matched the Additional Data, or (2) provide an indicator of the likelihood that the person attempting to use the deposit account was an accountholder. If a user of the services related to the Additional Data took "adverse action" (as defined by the FCRA) based on that information, the user would provide the individual with an adverse action notice in accordance with applicable law.

As a general matter, the Additional Data should be subject to the same rules under the FCRA and GLBA as have been imposed by PPS with respect to other data contributed to the NASD. However, a few specific points are worth mentioning.

1) The Additional Data should be used only for "permissible purposes" under the FCRA. This would include a retailer deciding whether to accept a check or initiate an ACH transaction in a sales transaction. However, it would not include marketing purposes.

2) The Additional Data is likely to be nonpublic personal information ("NPI") under the GLBA. In past discussions with Lisi and others, we have suggested that PPS adopt requirements that Contributors include in the GLBA privacy notices that they can share information "as permitted by law" (which presumably most if not all already do). This is important to ensure that the Additional Data (and other data provided by Contributors) is not subject to the opt-out rules under the GLBA.

3) Presently, the FCRA procedures that PPS has adopted provide that PPS will provide a consumer with information about the deposit account that the consumer identifies upon request. In part because the data base was not set up with respect to individuals, PPS did not adopt a procedure to provide the consumer with information about all deposit accounts that the consumer may have in the database. New procedures are likely to be required to provide all information on a consumer when an inquiry is received by the consumer. Among other things, PPS will need to consider how it will handle joint accounts.

4) Likewise, PPS's FCRA procedures adopted special steps to be taken to verify the identity of a consumer who requests to see his or her file at PPS because the files were organized by account number and the account holders were not known. Those procedures will need to be revised as the database is revised to include the Additional Data and it will be easier to identify the individual who is requesting to see PPS's file.

The foregoing are the primary impacts we have been able to identify under the federal FCRA with respect to the Project. Please call either [REDACTED] or me [REDACTED] with any questions or comments on the draft FAQs and the items noted above. We can discuss the extent to which PPS wants to consider additional issues under state law.

Jim

<<603957_21_.doc>>

"<mail.sidley.com>" made the following
annotations on 11/29/2002 08:44:35 AM

This e-mail is sent by a law firm and may contain information that is privileged or

confidential. If you are not the intended recipient, please delete the e-mail and any attachments and notify us immediately.

=====
==